

ПОЕДНАННЯ ЗАВАДОСТІЙКОГО КОДУВАННЯ ТА ШИФРУВАННЯ

Дубров О.

Науковий керівник – к.т.н., доцент Семеренко В.П.

Багатоканальні телекомунікаційні системи мають забезпечувати як секретність, так і надійність інформації, що передається. Запропоновано багато алгоритмів, що дозволяють збільшити завадостійкість і захищеність інформації при роздільному виконанні даних процедур.

Пропонується алгоритм одночасного кодування та шифрування інформації з низькими обчислювальними затратами на основі несистематичного кодування та гамування.

При несистематичному кодуванні кодове слово виходить у вигляді добутку інформаційного полінома на твірний:

$$c(x) = m(x)g(x)$$

При декодування виконується зворотна операція до множення та отримується декодований інформаційний вектор. Якщо при діленні виникла ненульова остача, то вона вказуватиме не тільки на наявність помилки, а й на розряд, що модифікувався в результаті завад або навмисного спотворення.

Вектор вхідної інформації кодується несиметричним кодом, тобто перевірочні символи явно не виділені. Це вже створює певний захист інформації, але його легко подолати. Для здійснення справжнього захисту після кодування вводимо гамування. Для цього використовуємо генератор псевдовипадкових чисел на регістрі зсуву з лінійним оберненим зв'язком. Для прикладу береться твірний поліном, що обов'язково має бути незвідним.

$$P(x) = x^{31} + x^{28} + x^{24} + x^4$$

Пристрій умовно можна поділити на передавальну і та приймальну частини. У кожній частині встановлені однакові генератори ПВП та суматори по модулю 2. У приймачу блок кодер замінений на декодер. У приймачу також передбачений блок виправлення помилок. Цей блок буде спрацьовувати тільки тоді коли помилка буде виявлена.

Проведено статистичні дослідження закодованої послідовності за допомогою спеціальних тестів, запропонованих лабораторією NIST, а саме: частотні побітові і блочні тести, також тест послідовностей біт.

Отже, запропонований метод забезпечує потрібне завадостійке кодування при високому рівні захисту інформації і одночасному спрощенні обчислень.